Exhibit B

STEPHEN KATTE MAR 06, 2023

7 DeFi protocol hacks in Feb see $21 million in funds stolen: DefiLlama

DeFi platforms lost over $21 million to hackers throughout February, according to data released by DeFi project aggregator DefiLlama.

Reentrancy, price oracle attacks and exploits across seven protocols caused the decentralized finance (DeFi) space to bleed at least $21 million in crypto in February.

According to DeFi data analytics platform DefiLlama, one of the largest in the month was the flash loan reentrancy attack on Platypus Finance, which led to $8.5 million of funds lost.

DefiLlama highlighted six other noteworthy hacks in the month, the first being the price oracle attack on BonqDAO on Feb 1.

LaunchZone	27 Feb, 2023		Protocol Logic	Access Control Exploit	$0.7m
Dexible	20 Feb, 2023		Protocol Logic	Arbitrary External Call	$2m
Hope Finance	20 Feb, 2023		Rugpull	Router Exploit	$1.86m
Platypus Finance	16 Feb, 2023		Ecosystem	Flashloan Reentrancy Attack	$8.5m
dForce Network	10 Feb, 2023		Protocol Logic	Reentrancy	$3.65m
Orion	2 Feb, 2023		Protocol Logic	Reentrancy	$3m
BonqDAO	1 Feb, 2023		Protocol Logic	Price Oracle Attack	$1.7m

DeFi platforms suffered seven attacks throughout February. Source: DefiLlama

BonqDAO: $1.7 million

BonqDAO revealed to its followers in a Feb. 1 post that its Bonq protocol was exposed to an oracle attack that allowed the exploiter to manipulate the price of the AllianceBlock (ALBT) token.

The exploiter increased the ALBT price and minted large amounts of Bonq Euro (BEUR). The BEUR was then swapped for other tokens on Uniswap. Then, the price decreased to almost zero, which triggered the liquidation of ALBT.

Blockchain security firm PeckShield estimated the losses to be around $120 million; however, it was later revealed hackers reportedly only cashed out around $1 million due to a lack of liquidity on BonqDAO.

Orion Protocol: $3 million

Just a day later, on Feb. 2, decentralized exchange Orion Protocol suffered a loss of roughly $3 million through a reentrancy attack, where attackers used a malicious smart contract to drain funds from a target with repeated withdrawal orders.

Alexey Koloskov · Feb 2, 2023
@alexeykoloskov · **Follow**
Replying to @alexeykoloskov

Instead of relying on low-impact bounty programs, our own funds were used in our smart contracts as a way to attract Web3's most sophisticated hackers. Of course, we always hoped that a vulnerability would not be found.

Alexey Koloskov
@alexeykoloskov · **Follow**

We have been investigating this very sophisticated attack from the minutes it occurred. We will not reopen the Deposit function until we feel confident that the bug has been fixed which will only be after successfully passing new audits from leading audit firms.

4:08 PM · Feb 2, 2023

18 Reply Share

Read 1 reply

Orion Protocol CEO Alexey Koloskov confirmed the attack at the time, assuring everyone that "All users' funds are safe and secure."

"We have reasons to believe that the issue was not a result of any shortcomings in our core protocol code but rather might have been caused by a vulnerability in mixing third-party libraries in one of the smart contracts used by our experimental and private brokers," he said.

DForce Network: $3.65 million

DeFi protocol dForce network was another February victim of a reentrancy attack resulting in around $3.65 million in losses.

In a Feb. 10 post, dForce confirmed the exploit; however, in a twist, all funds were returned when the attacker came forward as a white hat hacker.

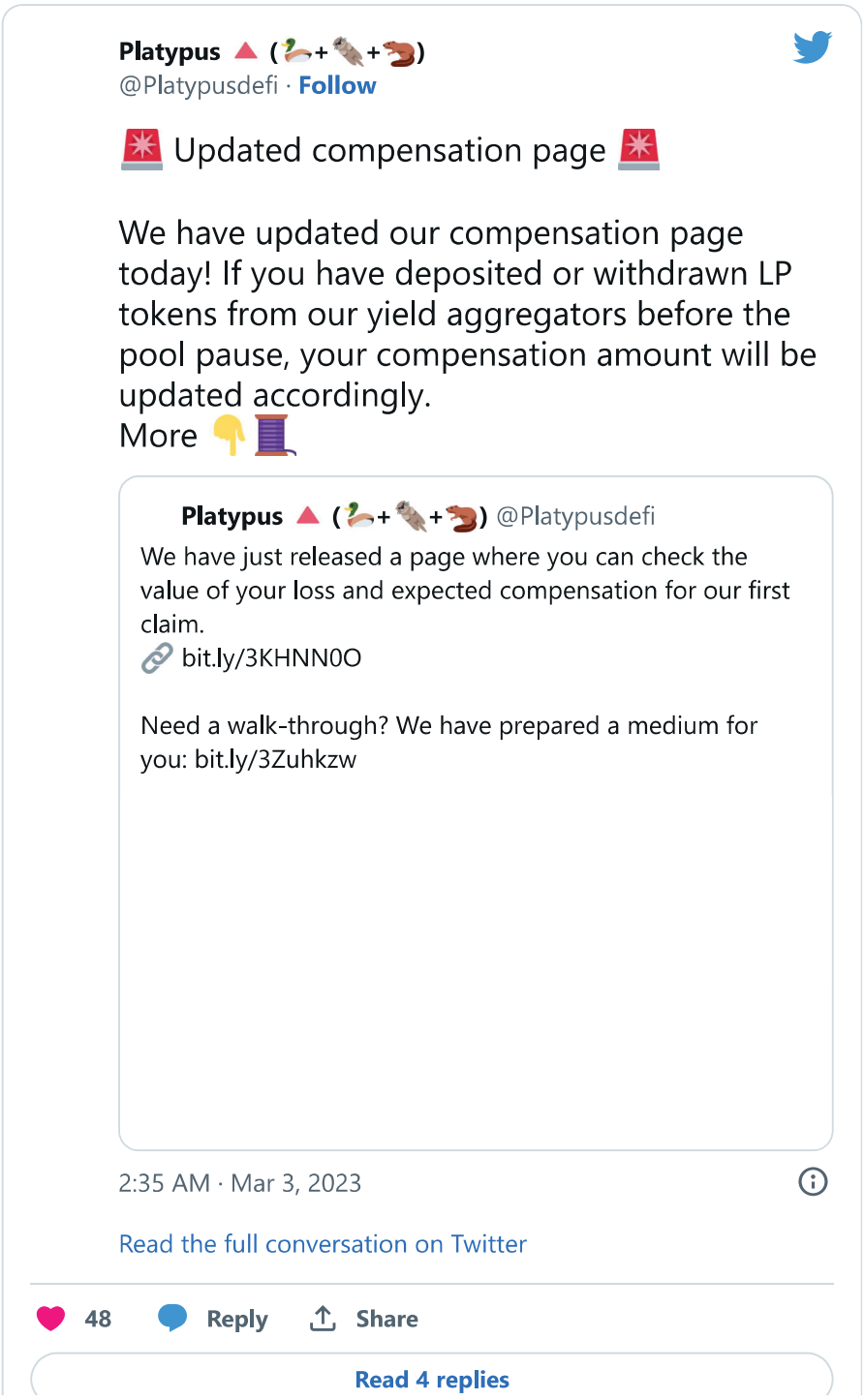
"On Feb. 13, 2023, the exploited funds were fully returned to our multisig on both Arbitrum and Optimism, a perfect ending for all," dForce said.

Platypus Finance: $9.1 million

On Feb. 16, DeFi protocol Platypus Finance suffered a flash loan attack resulting in $8.5 million being drained from the protocol.

A post-mortem report from Platypus auditor Omniscia noted that the attack was possible because of code in the wrong order.

On Feb. 23, the team announced that they are seeking to return around 78% of the main pool funds by reminting frozen stablecoins.



The team also confirmed second and third incidents, which led to another $667,000 exploited, bringing total losses to around $9.1 million.

French police arrested two suspects related to the hack and seized around $222,000 worth of crypto assets on Feb. 25.

Hope Finance: $1.86 million

A few days later, on Feb. 20, users of Arbitrum-based algorithmic stablecoin project Hope Finance fell prey to a smart contract exploit, which saw roughly $2 million stolen from users.

CertiK Alert
@CertiKAlert · **Follow**

#CommunityAlert 🚨

@hope_fin have announced the community has been scammed for ~$2m making this the largest #exitscam on Arbitrum in 2023.

$1.86m was transferred to @TornadoCash.

Hope_fin have posted steps for user's to withdraw their staked LP

> **Hope Finance (💙,🧡)** @Hope_fin
> Steps to withdraw your staked LP from the this fucking scam protocol
>
> 1. Go on this link
> arbiscan.io/address/0x1fc2...
>
> 2. connect your wallet
> 3. click on emergency withdraw
>
> Enter
> 0000000000000000000000000000000000000000000000000000000002

2:38 AM · Feb 21, 2023

14 Reply Share

Read more on Twitter

Web3 security firm CertiK flagged the incident on Feb. 21, following an announcement from the Hope Finance Twitter account notifying users of the scam.

A member of the CertiK team told Cointelegraph at the time that the scammer had changed the details of the smart contract, which led to funds being drained from Hope Finance genesis protocol:

> "It appears that the scammer changed the TradingHelper contract which meant that when 0x4481 calls OpenTrade on the GenesisRewardPool the funds are transferred to the scammer."

Dexible: $2 million

Multichain exchange aggregator Dexible was hit by an exploit that targeted the app's selfSwap function, with $2 million worth of cryptocurrency lost due to the Feb. 17 attack.

According to a Feb. 18 post from the exchange, "a hacker exploited a vulnerability in our newest smart contract. This allowed the hacker to steal funds from any wallet that had an unspent spend approval on the contract."

After investigating, the Dexible team found the attacker had used the app's selfSwap function to move over $2 million worth of crypto from users that had previously authorized the app to move their tokens.

After receiving the tokens into their own smart contract, the attacker withdrew the coins through Tornado Cash into unknown BNB BNB ▲ $337 wallets.

LaunchZone: $700,000

BNB Chain-based DeFi protocol LaunchZone had $700,000 worth of funds drained on Feb. 27.

According to blockchain security firm Immunefi, an attacker leveraged an unverified contract to drain the funds.

"An approval had been made to the unverified contract 473 days ago by the LaunchZone deployer," Immunefi said.

Related: Crypto exploit losses in January see nearly 93% year-on-year decline

The February figures are a stark increase from January, according to DefiLlama figures.

The tracker lists only $740,000 in hacks to DeFi platforms in the month across two protocols — Midas Capital and Roe Finance.

In its 2023 Crypto Crime Report, blockchain data firm Chainalysis revealed that hackers stole $3.1 billion from DeFi protocols in 2022, accounting for more than 82% of the total amount stolen in the year.

#Hackers #Cybercrime #Cybersecurity #Hacks #Data #DeFi

Add reaction

RELATED NEWS

What are gift card scams, and how to avoid them?

Blockchain for a better society: How to reach beyond financial inclusivity